

1C780 U.S. PTO
09/591927
06/12/00

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 6月21日

出願番号

Application Number:

平成11年特許願第174066号

出 願 人

Applicant (s):

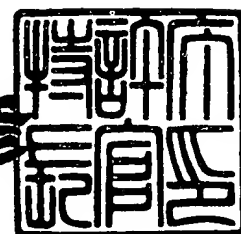
株式会社日立製作所

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

2000年 2月18日

特許庁長官
Commissioner,
Patent Office

近藤隆彦



出証番号 出証特 2000-3007551

【書類名】 特許願

【整理番号】 PNT990345

【提出日】 平成11年 6月21日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 19/00

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共情報事業部内

 【氏名】 三浦 淳一

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共情報事業部内

 【氏名】 斎藤 由紀夫

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共情報事業部内

 【氏名】 小磯 良太

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100061893

 【弁理士】

 【氏名又は名称】 高橋 明夫

 【電話番号】 03-3661-0071

【選任した代理人】

 【識別番号】 100086656

 【弁理士】

 【氏名又は名称】 田中 恭助

【電話番号】 03-3661-0071

【手数料の表示】

【予納台帳番号】 011626

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子認証方法及びプログラム格納媒体

【特許請求の範囲】

【請求項 1】

サービスを要求する側の第 1 の計算機とサービスを提供する側の第 2 の計算機とがネットワークを介して接続され、第 2 の計算機から第 1 の計算機へ要求されたコンテンツを送信し、該コンテンツに関して第 1 の計算機から第 2 の計算機へデータを送信するシステムの電子認証方法において、

第 2 の計算機によって該コンテンツのアクセス対応にアクセス番号を生成して記憶装置に登録するとともに該コンテンツ内に該アクセス番号を視覚不可なように埋め込んで第 1 の計算機へ送信し、第 1 の計算機によって該コンテンツを表示し、該コンテンツに関して入力されたデータに該コンテンツから取り出した該アクセス番号を付加して第 2 の計算機へ送信し、第 2 の計算機によつて受信した該アクセス番号が登録済であるときに受信したデータの正当性を認証するとともに登録された該アクセス番号を無効にすることを特徴とする電子認証方法。

【請求項 2】

第 2 の計算機は、さらに該コンテンツのアクセス対応に公開鍵と秘密鍵を生成して記憶装置に登録するとともに該コンテンツ内に該公開鍵を視覚不可なように埋め込んで第 1 の計算機へ送信し、第 1 の計算機によって該コンテンツに関して入力されたデータを該コンテンツから取り出した該公開鍵によって暗号化して第 2 の計算機へ送信し、第 2 の計算機によって受信した該アクセス番号が登録済であるときに登録された該秘密鍵によって受信したデータを復号することを特徴とする請求項 1 記載の電子認証方法。

【請求項 3】

計算機読み取り可能なプログラムを格納する記憶媒体であって、該プログラムは、外部から要求されたコンテンツのアクセス対応にアクセス番号を生成する機能と、生成されたアクセス番号を記憶装置に登録する機能と、該コンテンツ内に該アクセス番号を視覚不可なように埋め込んで外部へ送信する機能と、外部から該アクセス番号を付加したデータを受信する機能と、受信した該アクセス番号が

登録済であるときに受信したデータの正当性を認証するとともに、登録された該アクセス番号を無効にする機能とを有することを特徴とするプログラムの記憶媒体。

【請求項 4】

前記プログラムは、さらに該コンテンツのアクセス対応に公開鍵と秘密鍵を生成する機能と、生成された公開鍵と秘密鍵を記憶装置に登録する機能と、該コンテンツ内に該公開鍵を視覚不可なように埋め込んで外部へ送信し、外部から該公開鍵によつて暗号化された該データを受信する機能と、受信した該アクセス番号が登録済であるときに登録された該秘密鍵によつて受信したデータを復号する機能とを有することを特徴とする請求項 3 記載のプログラムの記憶媒体。

【請求項 5】

計算機読み取り可能なプログラムを格納する記憶媒体であつて、該プログラムは、外部から受信したコンテンツを表示する機能と、該コンテンツに関してデータ入力を受ける機能と、該コンテンツ内に視覚不可なように埋め込まれたアクセス番号を取り出す機能と、入力された該データに該アクセス番号を付加して外部へ送信する機能とを有することを特徴とするプログラムの記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、サービスを提供する側の計算機からサービスを要求する側の計算機へコンテンツを送信し、このコンテンツに関して後者の計算機から前者の計算機へ入力データを送信するシステムに係わり、特に正当なコンテンツアクセスに関する入力データであることを認証する電子認証方法に関する。

【0002】

【従来の技術】

インターネットを利用する電子商取引の分野では、本人認証、データの改ざん防止等のセキュリティ技術が重要である。従来のセキュリティ技術としてパスワード方式、データを暗号化するための種々の暗号化方式、電子証明書発行など様々な努力が払われてきた。例えばインターネット上でクレジットカード決済を安

全に行うプロトコル仕様であるSET (Secure Electronic Transactions)、ベリサイン社の電子認証システムなどを挙げることができる。

【0003】

【発明が解決しようとする課題】

インターネットを利用するシステムでは、一般にクライアントがWWW (World Wide Web) サーバにコンテンツを要求し、WWWサーバがクライアントへ要求されたコンテンツを送信し、クライアントが受信したコンテンツを表示装置上に表示する。クライアントがこのコンテンツに関してデータを入力し、入力されたデータをWWWサーバへ送信すると、WWWサーバが受信したデータの処理を実行する。ここでクライアント側でコンテンツのコピーが容易であるため、コンテンツのコピーを採取しておいて再利用し、許可されていないデータをWWWサーバへ送信したり、他人がコンテンツ画面を介して入力したデータを改ざんしてWWWサーバへ送信するといった不正が発生する可能性がある。

【0004】

本発明の目的は、提供されるコンテンツに対して応答されるデータが正当なコンテンツアクセスに関する入力データであることを認証する方法を提供することにある。

【0005】

また本発明の他の目的は、このような電子認証方法を実現するためのプログラムを格納する記憶媒体を提供することにある。

【0006】

【課題を解決するための手段】

本発明は、サービスを要求する側の第1の計算機とサービスを提供する側の第2の計算機とがネットワークを介して接続され、第2の計算機から第1の計算機へ要求されたコンテンツを送信し、該コンテンツに関して第1の計算機から第2の計算機へデータを送信するシステムの電子認証方法において、第2の計算機によってコンテンツのアクセス対応にアクセス番号を生成して記憶装置に登録するとともにこのコンテンツ内にそのアクセス番号を視覚不可なように埋め込んで第

1の計算機へ送信し、第1の計算機によってこのコンテンツを表示し、このコンテンツに関して入力されたデータにコンテンツから取り出したアクセス番号を付加して第2の計算機へ送信し、第2の計算機によつて受信したそのアクセス番号が登録済であるときに受信したデータの正当性を認証するとともに登録されたアクセス番号を無効にする電子認証方法を特徴とする。

【0007】

また本発明は、上記方法を第1の計算機で実行されるプログラム又は第2の計算機で実行されるプログラムとして格納する記憶媒体を特徴とする。

【0008】

【発明の実施の形態】

以下、本発明の一実施形態について図面を用いて説明する。

【0009】

図1は、本実施形態のインターネットを利用してサービスを提供するシステムの構成図である。システムはクライアント1、WWWサーバ2及び両者を接続するネットワークであるインターネット3から構成される。クライアント1は、サービス要求を発行しサービスを受ける側のパソコンなどの計算機であり、その処理装置には、表示装置11及び入力装置12が接続される。またそのメモリにはWWWブラウザ13が格納され、処理装置によって実行される。表示装置11はコンテンツの内容を表示する装置、入力装置12はデータ及び指令を入力する装置である。WWWブラウザ13は、インターネット3を介してWWWサーバ2へコンテンツを要求し、得られたコンテンツを表示装置11に表示する。また入力装置12を介して入力されたデータをWWWサーバ2へ送信する。

【0010】

WWWサーバ2は、サービスを提供する側の計算機であり、その処理装置に接続される記憶装置上にアクセス管理テーブル21及びコンテンツDB（データベース）22を格納する。アクセス管理テーブル21は、コンテンツへのアクセスを管理するための認証情報を格納する。コンテンツDB22は、クライアント1に提供するコンテンツを格納するDBである。ここでコンテンツとは、WWWサーバ2に蓄積されクライアント1に提供される表示画面情報であり、テキストデ

ータ、イメージデータ、静止画、動画などのうち少なくとも1つを含む情報である。WWWサーバ2のメモリに格納されその処理装置で実行されるWWWサーバプログラム23は、クライアント1の要求に従ってクライアント1へコンテンツを送信するとともに、各コンテンツ要求ごとにアクセス管理テーブル21に認証情報を格納し、そのコンテンツに係わるクライアント1から送られるデータの認証を行う。

【0011】

なお本発明の電子認証機能を含むWWWサーバプログラム23を記憶媒体に格納して、WWWサーバ2の駆動装置を介してWWWサーバ2のメモリに読み込むか、ネットワークを介する伝送によってWWWサーバ2へ伝送し、WWWサーバ2のメモリに格納してWWWサーバ2の処理装置によって実行することが可能である。本発明の電子認証機能を含むWWWブラウザ13についても同様に、そのプログラムを記憶媒体に格納して、クライアント1の駆動装置を介してクライアント1のメモリに読み込むか、ネットワークを介する伝送によってクライアント1へ伝送し、クライアント1のメモリに格納してクライアント1の処理装置によって実行することが可能である。

【0012】

図2は、アクセス管理テーブル21を構成する各アクセス情報レコードのデータ形式を示す図である。同レコードは、アクセス番号41、公開鍵42、秘密鍵43および登録日時44の各項目から構成される。アクセス番号41はコンテンツにアクセスするごとに生成され、そのコンテンツアクセスに付随する番号である。公開鍵42はそのコンテンツに関してクライアント1から送信されるデータの機密を保護するために生成される暗号鍵である。秘密鍵43は公開鍵42によって暗号化された暗号文を復号するための復号鍵である。アクセス番号41、公開鍵42及び秘密鍵43は、コンテンツアクセスごとに生成される。登録日時44は当該アクセス情報レコードが登録された日時（日付、時刻）である。

【0013】

図3A及び図3Bは、クライアント1のWWWブラウザ13及びWWWサーバ2のWWWサーバプログラム23の処理の流れを示すフローチャートである。W

WWWブラウザ 1 3 が WWWサーバ 2 へコンテンツ要求を送信すると（ステップ 5 1）、WWWサーバプログラム 2 3 はこのコンテンツ要求を受信する（ステップ 5 2）。次に乱数を発生させてアクセス番号を採番し（ステップ 5 3）、また公開鍵暗号方式に従って公開鍵及びその秘密鍵を生成する（ステップ 5 4）。次にコンテンツ DB 2 2 を検索して要求されたコンテンツを取り出し（ステップ 5 5）、電子透かしの技術を用いてそのコンテンツに生成したアクセス番号と公開鍵をユーザによって視覚できないように埋め込む（ステップ 5 6）。これらの情報を埋め込むコンテンツ上の位置としては、位置決めの便のためにインターネットマーク、ロゴマークなど特定のマークを包含する矩形領域が望ましい。また電子透かしの技術の適用の容易性からみて濃淡画像領域が望ましい。次に生成したアクセス番号 4 1、公開鍵 4 2 及び秘密鍵 4 3 に登録日時 4 4 を加えて新しいアクセス情報レコードとしてアクセス管理テーブル 2 1 に登録する（ステップ 5 7）。次にこのようにして認証情報を埋め込んだコンテンツをクライアント 1 へ送信する（ステップ 5 8）。

【 0 0 1 4 】

WWWブラウザ 1 3 は、このコンテンツを受信し（ステップ 5 9）、表示装置 1 1 上に表示する（ステップ 6 0）。ここでコンテンツはユーザが視覚できるように表示されるが、埋め込まれたアクセス番号と公開鍵は表示されず、ユーザは視覚によって認識できない。入力装置 1 2 を介してデータが入力されたとき（ステップ 6 1）、図 3 B に移り、WWWブラウザ 1 3 は、コンテンツから電子透かしが埋め込まれている位置を取得し、埋め込まれたアクセス番号と公開鍵を取り出す（ステップ 6 2）。次に入力されたデータをこの公開鍵によって暗号化して電文を作成し（ステップ 6 3）、この電文にアクセス番号を付加してWWWサーバ 2 へ送信する（ステップ 6 4）。アクセス番号を暗号化してもよいが、秘密性が少ないので特に暗号化する必要はない。

【 0 0 1 5 】

WWWサーバプログラム 2 3 はこの電文を受信し（ステップ 6 5）、受信したアクセス番号によってアクセス管理テーブル 2 1 を検索する（ステップ 6 6）。該当するアクセス情報レコードが存在すれば（ステップ 6 7 Y E S）、電文の暗

号化されている部分を秘密鍵によって復号化する（ステップ68）。該当するアクセス情報レコードが存在しなければ（ステップ67NO）、受信した電文を破棄する（ステップ69）。次に復号化されたデータがあらかじめ予想される意味のあるデータか否かによつて復号化できたか否かを判定する（ステップ70）。復号化できた場合（ステップ70YES）には、当該アクセス情報レコードをアクセス管理テーブル21から削除し（ステップ71）、受信したデータに基づいて以降の処理を実行する（ステップ72）。復号化できない場合（ステップ70NO）には、受信した電文を破棄し（ステップ73）、当該アクセス情報レコードをアクセス管理テーブル21から削除する（ステップ74）。以降の処理は行わない。アクセス情報レコードの削除は、一般的にはそのレコードを無効にするということになる。

【0016】

なおWWWサーバ2は、周期的にアクセス管理テーブル21に登録されたアクセス情報レコードの登録日時44をチェックし、所定時間以上経過したアクセス情報レコードをアクセス管理テーブル21から削除する。これによってデータ入力による応答のないコンテンツアクセスの認証を中止する。

【0017】

上記実施形態によれば、クライアント1へ送られるコンテンツにはアクセス番号が埋め込まれ、このアクセス番号はコンテンツアクセスごとに生成されるので、このコンテンツをコピーしてデータ入力し、WWWサーバ2へ送信してもすでにそのアクセス番号はWWWサーバ2によって無効化されていることになり、WWWサーバ2へ送信されるデータは無効となる。またクライアント1からインターネット3を介してWWWサーバ2へ電文を送信する途中でアクセス番号が盗聴されたとしてもそのアクセス番号を再利用しようとすると無効となる。クライアント1のユーザがコンテンツに埋め込まれているアクセス番号を解読しても同様であり、他の目的のために再利用できない。

【0018】

また上記実施形態によれば、クライアント1へ送られるコンテンツには1回使用に限定される公開鍵が埋め込まれているので、クライアント1からWWWサー

バ2へ送られる個人情報など秘密性のある情報を保護することができる。この公開鍵によって暗号化された情報が盗聴されたとしても再利用できず、従って他人の個人情報を盗聴して本人になりすましたり、他人の注文書の金額、数量などを改ざんするなどの不正を防止できる。

【0019】

上記実施形態では電子透かしの技術を利用するが、その主たる目的は、アクセス番号及び公開鍵はコンテンツの内容ではなくユーザに知らせる必要がないので電子透かしの方法を用いて隠しておくことにあり、特に電子透かしの方法に秘密性があるわけではない。従って電子透かしの方式は、多くのコンテンツに広く適用でき、WWWブラウザ13及びWWWサーバプログラム23に共通に適用できるように単純で確実に電子透かしを埋め込める方式が望ましい。

【0020】

また上記実施形態では、WWWサーバ2は乱数発生によってアクセス番号を生成したが、コンテンツの著作権保護など他の目的にも利用するためにアクセス番号の生成を連番（通し番号）としてもよい。ただしアクセス番号を連番とすると、コンテンツ中のアクセス番号の解読によって将来のコンテンツアクセスの際に生成されるアクセス番号が予想される危険性がある。またアクセス番号の桁数を多くとり、ハッシュ関数によってハッシュ値を求め、コンテンツ中にアクセス番号のハッシュ値を埋め込んでもよい。その場合にはアクセス番号41にはハッシュ値を格納し、ステップ66ではハッシュ値によってアクセス管理テーブル21を検索することになる。

【0021】

本発明により、インターネットを利用する電子商取引、インターネット・ショッピングなどにおいてWWWサーバ2からクライアント1へ送られたコンテンツに関してクライアント1からWWWサーバ2へ個人情報、取引データなどを送信する際にその個人情報、取引データなどが正当なコンテンツアクセスに関する入力データであることを証明できる。またユーザのミスによって1つの注文書に対して2つ以上の注文を発行するなど二重に取引データを送信するミスも防止できる。

【 0 0 2 2 】

【発明の効果】

以上述べたように本発明によれば、サーバがクライアントに提供するコンテンツにはアクセス番号が付随し、このコンテンツに関するサーバへの応答データにはアクセス番号が伴うため、1回のコンテンツアクセスに関する応答データは1回のみに限定することができ、コンテンツのコピーを利用する許可されていない応答データやデータの改ざんを目的とした不正な応答データを排除し、入力データが正当なコンテンツアクセスに関する応答データであることを認証できる。また応答データを1回限りの公開鍵によって暗号化することができ、応答データの盗聴を防止することができる。

【図面の簡単な説明】

【図 1】

実施形態のインターネットを利用してサービスを提供するシステムの構成図である。

【図 2】

実施形態のアクセス管理テーブル 2 1 のデータ構成を示す図である。

【図 3 A】

実施形態のシステムの処理の流れを示すフローチャートである。

【図 3 B】

実施形態のシステムの処理の流れを示すフローチャート（続き）である。

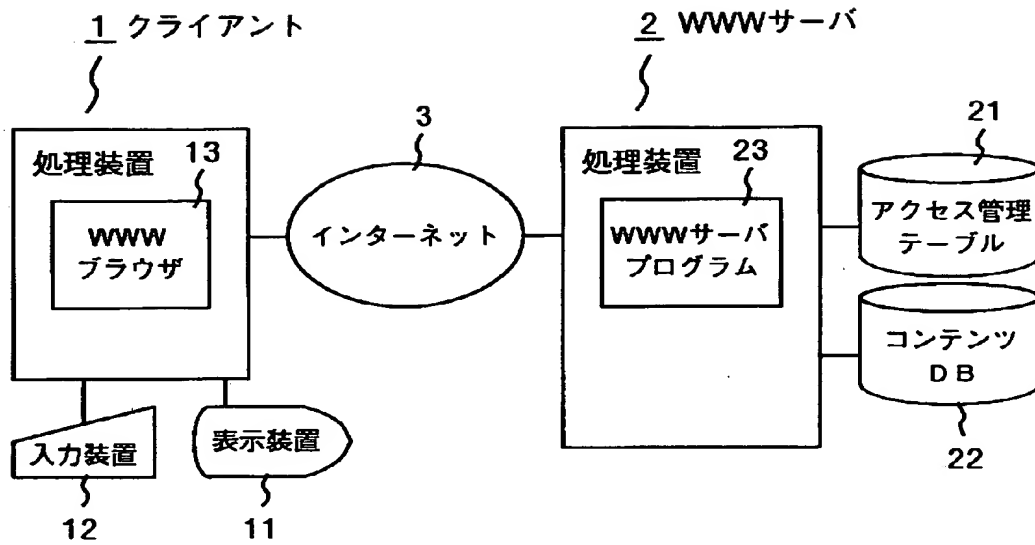
【符号の説明】

1 : クライアント、2 : WWWサーバ、3 : インターネット、1 3 : WWWブラウザ、2 1 : アクセス管理テーブル、2 2 : コンテンツDB、2 3 : WWWサーバプログラム、4 1 : アクセス番号、4 2 : 公開鍵、4 3 : 秘密鍵

【書類名】 図面

【図 1】

図 1



【図 2】

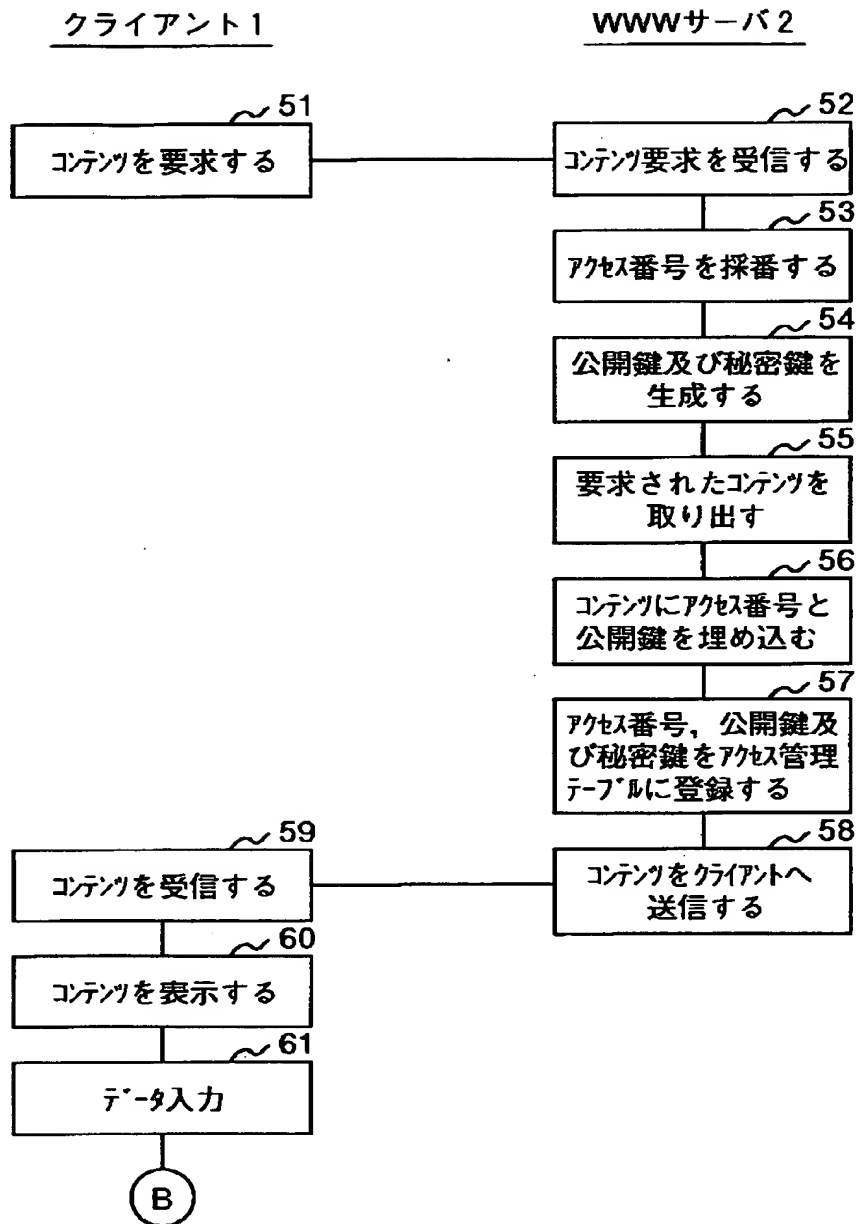
図 2

21 アクセス管理テーブル

41	42	43	44
アクセス番号	公開鍵	秘密鍵	登録日時

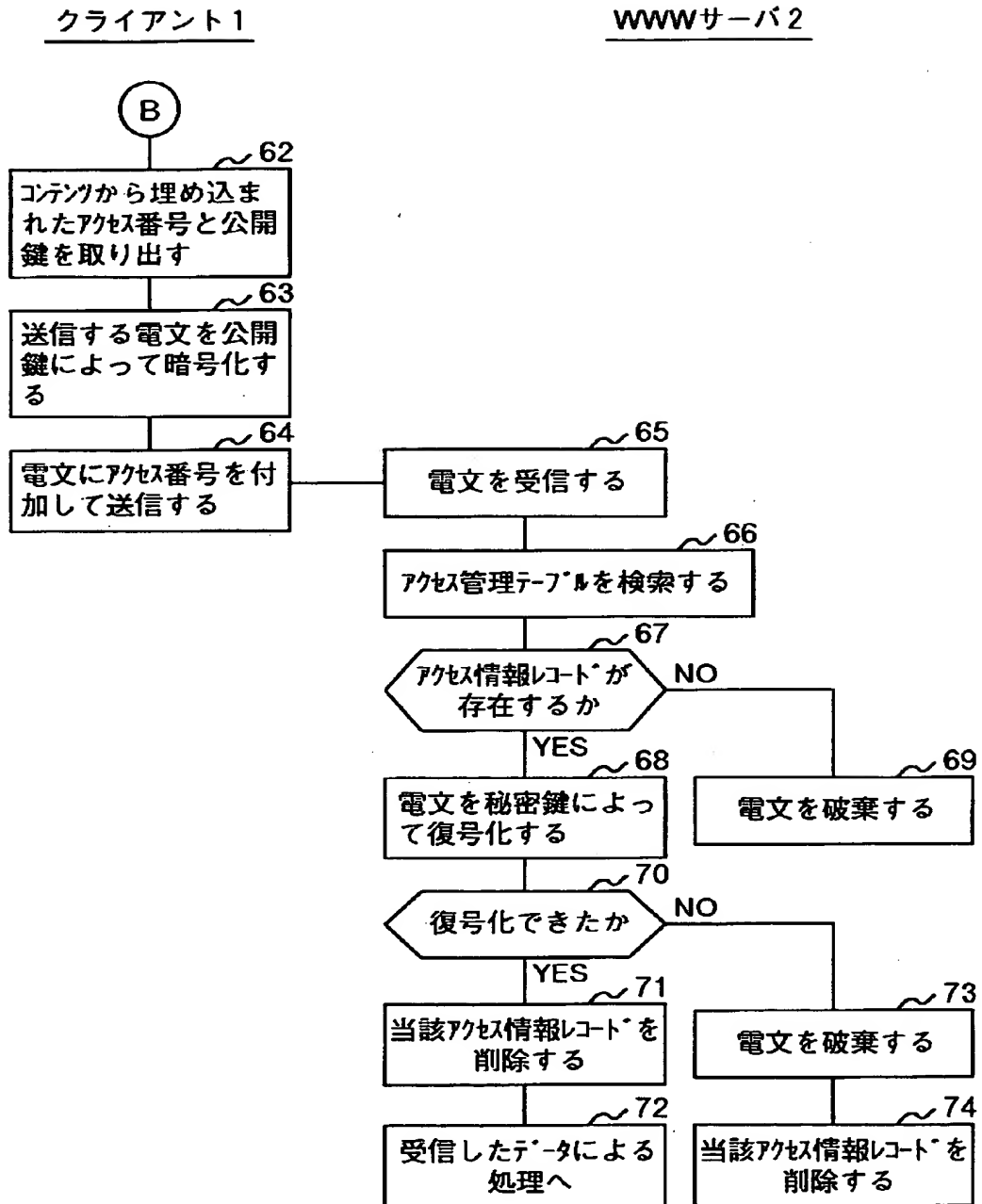
【図 3 A】

図 3 A



【図 3 B】

図 3 B



【書類名】 要約書

【要約】

【課題】 サーバからクライアントへ要求されたコンテンツを送信し、クライアントからサーバへこのコンテンツに関する入力データを送信するシステムにおいて、応答データが正当なコンテンツアクセスに関するデータであることを認証する。

【解決手段】 WWWサーバプログラム 2 3 は、コンテンツのアクセス対応にアクセス番号を生成してアクセス管理テーブル 2 1 に登録するとともに、このコンテンツ内にそのアクセス番号を埋め込んでクライアント 1 へ送信する。WWWブラウザ 1 3 は、このコンテンツを表示し、このコンテンツに関して入力されたデータにコンテンツから取り出したアクセス番号を付加してWWWサーバ 2 へ送信する。WWWサーバプログラム 2 3 は、受信したアクセス番号が登録済であるときに受信したデータの正当性を認証するとともに、登録されたアクセス番号を無効にする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号

[000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所